10

Fig. 1

Exploitation
Detection
Module
(1st Component)

12

INTERFACES
(Optional)

14

Forensics
Module
(2nd Component)

16

OS Restoration
Module
(3rd Component)

20

Start

22
Detect Occurrence
of Exploit

24
Collect Forensics Data That
is Characteristic of Exploit

26
Restore OS

End

Fig. 2

31
START

32
launch

12

34
Load/execute/
unload kernel
module
(main.c).

36
File Checker
(ls.pl)

38
Port Checker
(bc.pl)

39
END

FIG. 3

FIG. 4

SECURITY SOFTWARE SYSTEM

Hidden Module Detection Model	Anomaly →	Malicious kernel module memory range is reported	
System Call Table Integrity Verification Model	Anomaly →	Malicious kernel module memory range is reported	
Hidden Process Detection Model	Anomaly →	Malicious process ID and name is reported	
Hidden File Detection Model (File Checker)	Anomaly →	Malicious file listener is reported	
Hidden Port Detection Model (Port Checker)	Anomaly →	Malicious port location is reported	

INTERFACES

Forensics Module

OS Restoration Module

FIG. 5

KERNEL MODULE HIDING
Module list before removal

NULL → | prev | Module 1 | next | ↔ | prev | Module 2 | next | ↔ | prev | Module 3 | next | → NULL

FIG. 6(a)

Module list after hacker technique for removal

NULL → | prev | Module 1 | next | | prev | Hacker Module | next | | prev | Module 3 | next | → NULL

FIG. 6(b)

HIDDEN KERNEL MODULE DISCOVERY MODEL

0xFFFFFFFF

P
H
Y
S
I
C
A
L

M
E
M
O
R
Y

unused memory
for proper
alignment

Module 4 (0x1102 bytes size)   79

Hidden Hacker Module   78

Module 3 (0x1102 bytes size)   77

76

Module 2 (0xc102 bytes size)   75

74

73

Module 1 (0x2102 bytes size)

72

Kernel Memory   71

0xC0100000

BEST GUESS FOR NEXT
MODULE START POINT

$\sum$ previous module sizes
+
page size alignment
considerations

70

FIG. 7

USER SPACE MEMORY   94

```
/* ps.c application */
#include <stdio.h>

...

int main (int argc, char **argv) {
    DIR *dir;
    struct dirent *entry;

    dir = opendir("/proc");
    while ((entry = readdir(dir) != NULL) {
        ...
    }
}
```

INTERRUPT   90

SYSCALL Table

1	sys_exit
2	sys_fork
3	sys_read
4	sys_write
5	sys_open
6	sys_close
7	sys_waitpid
8	sys_creat
9	sys_link
10	sys_unlink

92

KERNEL SPACE MEMORY   96

```
/* kernel open.c */
long sys_open(const char *filename, int flags, int mode) {
    char *tmp;
    int fd, error;

    ...
}
```

FIG. 9

80

Initialization

81

Lock vmlist from
reading

82

For every vmlist
element

83

Module? —N

Y

84

Make a pointer to
the module

42

85

Valid Module? —N

Y

86   87

Hidden? —Y— Write results to the
output file

N

18

Forensics
Interface

Restoration
Interface

88

Lock vmlist from
reading

89

RETURN

FIG. 8

FIG. 10 (a)

101 START

102 Initialization

103 Obtain address of system call table

104 Check system call table

105 END

44

FIG. 10(b)

106 Initialization

107 for the first 50 bytes following the interrupt 80 location

108 is this a call to a double word pointer?

N

Y

109 RETURN

103

FIG. 10(c)

110 Initialization

111 for the entire size of the syscall table

112 out of range?

N

Y

113 Write results to the output file

Forensics Interface

Restoration Interface

18

114 set highest and lowest values

116 Are System Calls Patched?

Y

115 Search modules

N

117 RETURN

104

FIG. 10(d)

IDENTIFIED SYSCALL ANOMALIES CAUSE BY ADORE v0.42

```
syscall[2]    fork       FAILED     0xf8aca650
syscall[4]    write      FAILED     0xf8aca7e8
syscall[5]    open       FAILED     0xf8acb184  ──→ Highest
syscall[6]    close      FAILED     0xf8aca898
syscall[18]   oldstat    FAILED     0xf8acabe4
syscall[37]   kill       FAILED     0xf8aca710
syscall[39]   mkdir      FAILED     0xf8aca9a0
syscall[84]   oldlstat   FAILED     0xf8acacd0
syscall[106]  stat       FAILED     0xf8acadbc
syscall[107]  lstat      FAILED     0xf8acae94
syscall[120]  clone      FAILED     0xf8aca6b0
syscall[141]  getdents   FAILED     0xf8aca368  ──→ Lowest
syscall[195]  stat64     FAILED     0xf8acaf80
syscall[196]  lstat64    FAILED     0xf8acb080
syscall[220]  getdents64 FAILED     0xf8aca4d
```
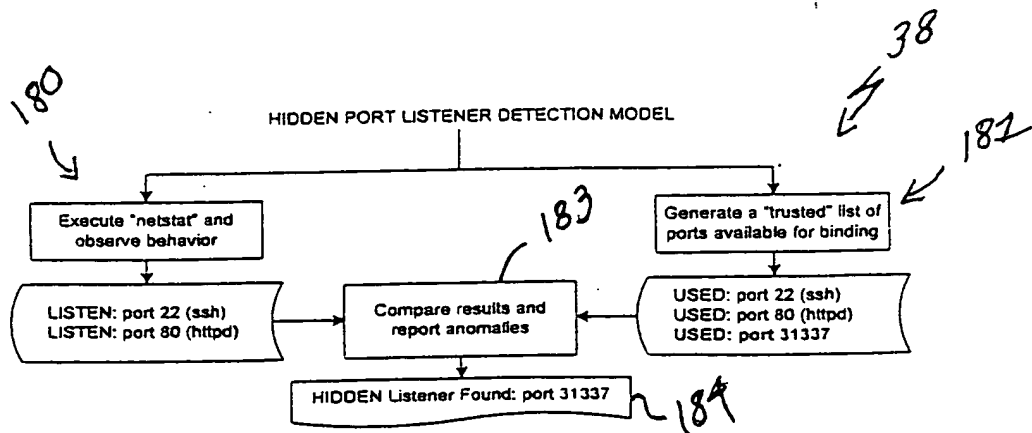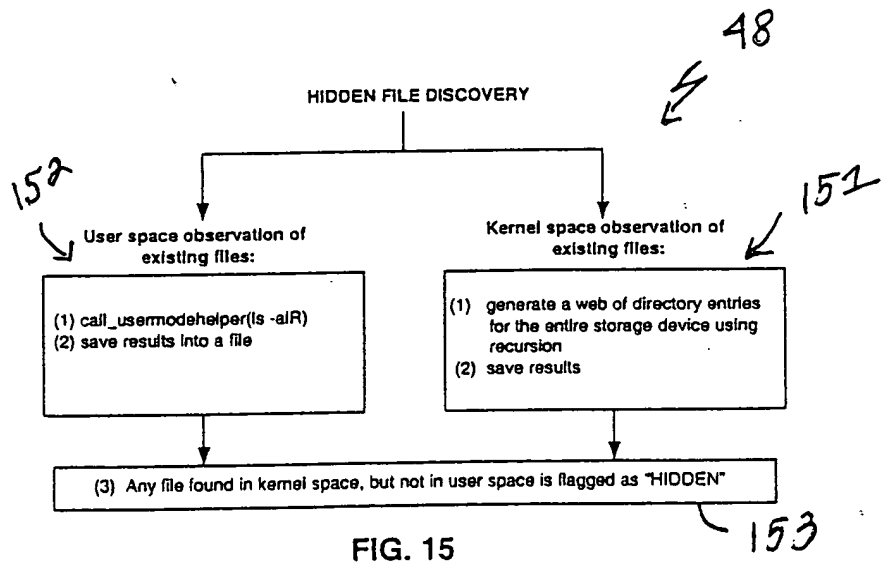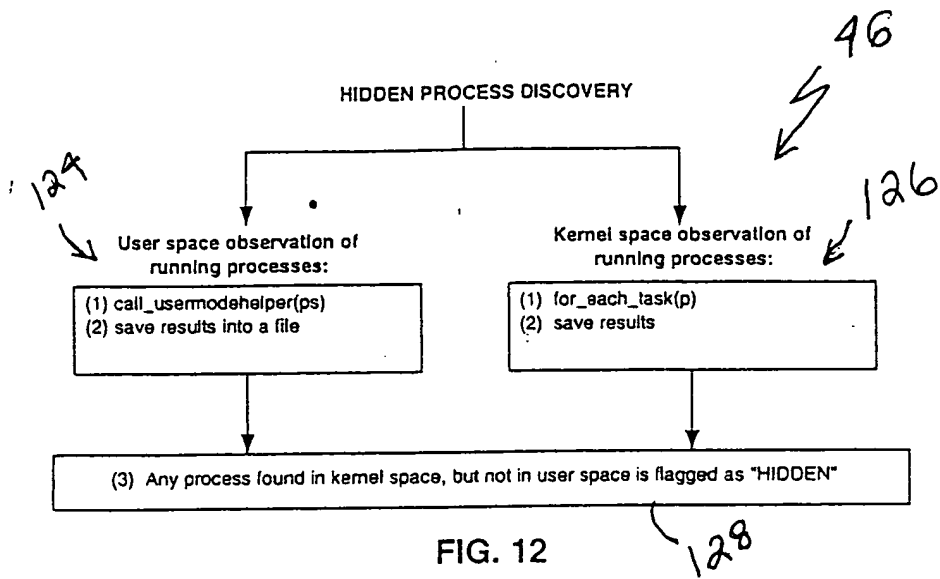
```
analyze_memory(highest, lowest) {

    if the range falls between two
    valid kernel modules then flag
    the entire memory range in
    between the two as a malicous
    kernel module.

}
```
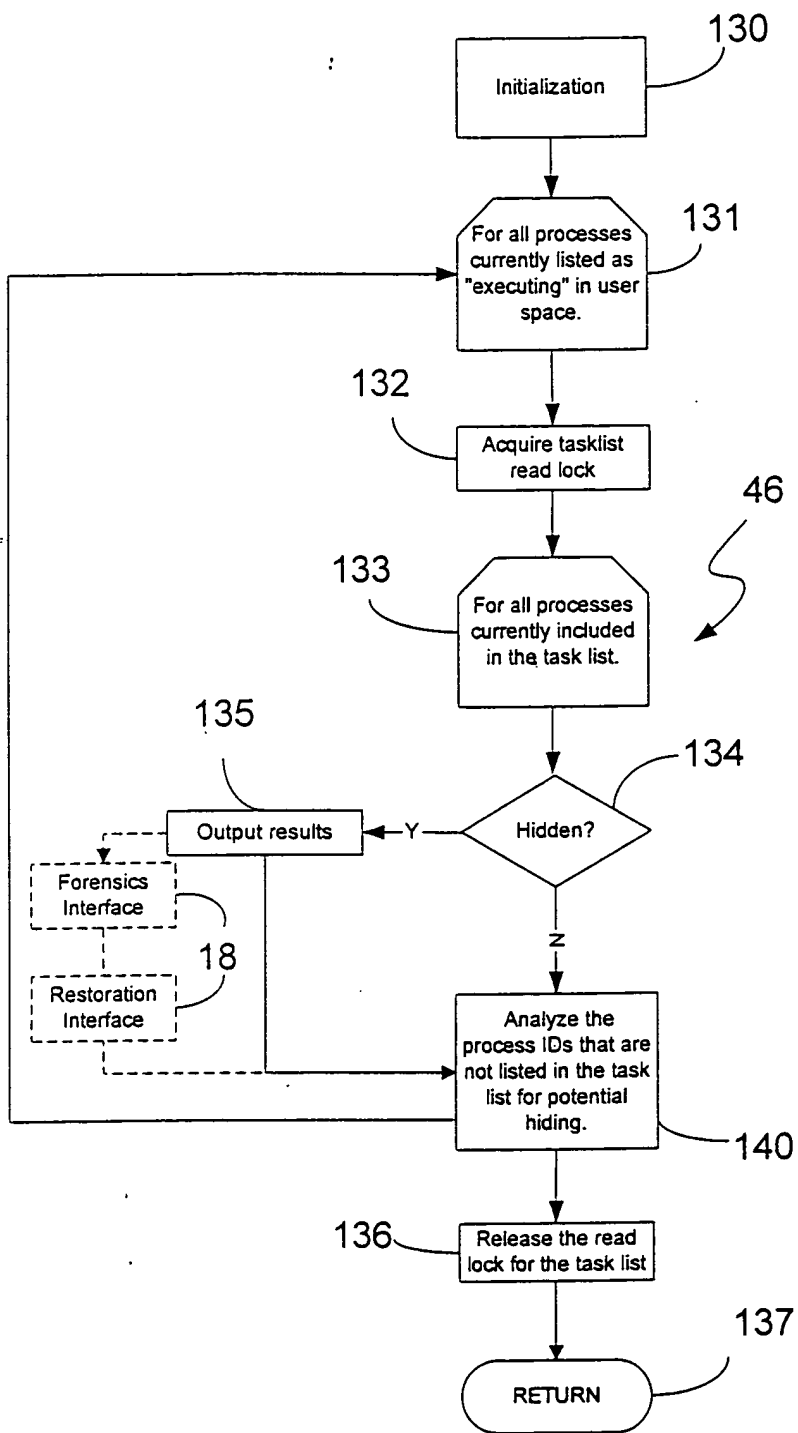
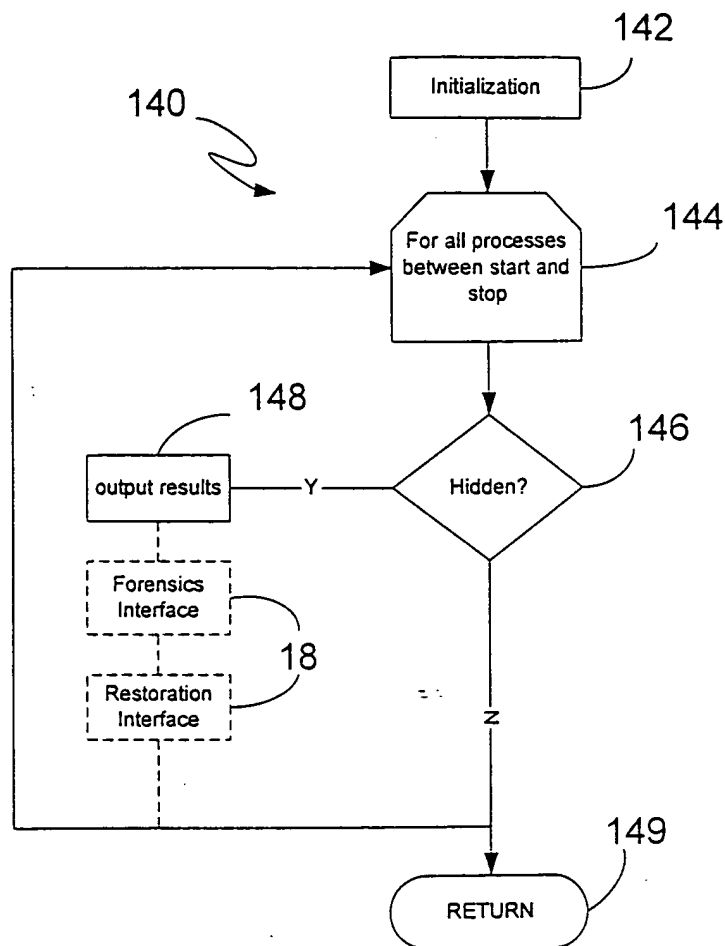FIG. 11
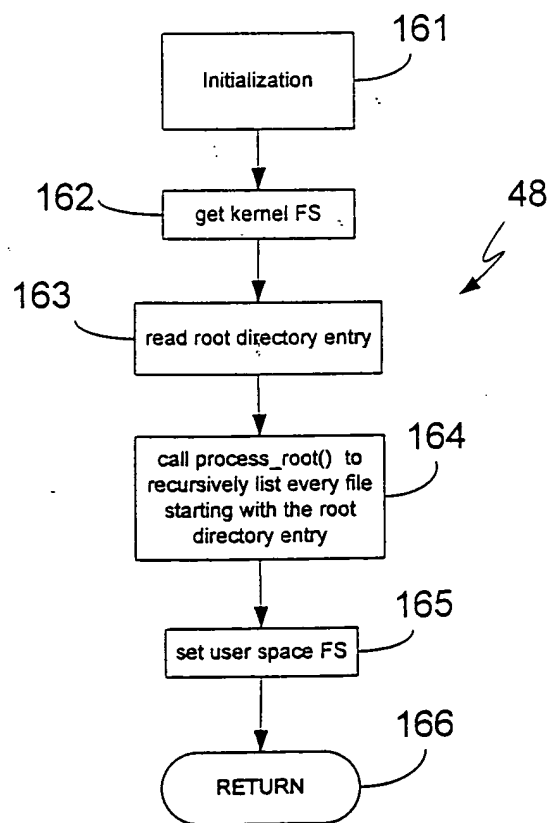
HIDDEN PROCESS DISCOVERY

46

124

126

User space observation of
running processes:

(1) call_usermodehelper(ps)
(2) save results into a file

Kernel space observation of
running processes:

(1) for_each_task(p)
(2) save results

(3) Any process found in kernel space, but not in user space is flagged as "HIDDEN"

FIG. 12

128

HIDDEN FILE DISCOVERY

48

152

151

User space observation of
existing files:

(1) call_usermodehelper(ls -alR)
(2) save results into a file

Kernel space observation of
existing files:

(1) generate a web of directory entries
for the entire storage device using
recursion
(2) save results

(3) Any file found in kernel space, but not in user space is flagged as "HIDDEN"

FIG. 15

153

HIDDEN PORT LISTENER DETECTION MODEL

38

180

182

Execute "netstat" and
observe behavior

Generate a "trusted" list of
ports available for binding

LISTEN: port 22 (ssh)
LISTEN: port 80 (httpd)

Compare results and
report anomalies

183

USED: port 22 (ssh)
USED: port 80 (httpd)
USED: port 31337

HIDDEN Listener Found: port 31337

184

FIG. 18

FIG. 13

Initialization — 130

For all processes currently listed as "executing" in user space. — 131

Acquire tasklist read lock — 132

For all processes currently included in the task list. — 133 / 46

Hidden? — 134

Output results — 135

Forensics Interface — 18
Restoration Interface — 18

Analyze the process IDs that are not listed in the task list for potential hiding. — 140

Release the read lock for the task list — 136

RETURN — 137

FIG. 13

FIG. 14

140

Initialization — 142

For all processes between start and stop — 144

output results — 148

Forensics Interface — 18
Restoration Interface — 18

Hidden? — 146

RETURN — 149

FIG. 14

FIG. 16

Initialization — 161

get kernel FS — 162

48

read root directory entry — 163

call process_root() to recursively list every file starting with the root directory entry — 164

set user space FS — 165

RETURN — 166

FIG. 16

Fig. 17

START — 170

Initialization — 171

For every file listed in the "trusted" results file — 172

173 — Exist?

Y

N — output results — 174

36

Forensics Interface

Restoration Interface — 18

END — 175

FIG. 19

START — 190

Initialization — 191

For every possible port — 192

193 — Bind?

Y

N

38

194 — Hidden?

N

output results — 195

Forensics Interface

Restoration Interface — 18

END — 196

```
Script started on Sat Aug  9 15:42:00 2003
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator_ this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

------------------------[ SUMMARY ]------------------------
NO hidden modules were found.
NO system call table modifications were found.
NO hidden processes were found.
WARNING: File size is 60133 (should be 58885): /var/log/sa/sa09
WARNING: File size is 1010871 (should be 1010003): /var/log/cron
WARNING: File size is 597700 (should be 597264): /var/log/maillog
NO hidden files were found.
NO hidden TCP port listeners were found.
[root@localhost interrogator]# exit
Script done on Sat Aug  9 16:01:52 2003
```

FIG. 20(a)

```
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator_ this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

------------------------[ SUMMARY ]------------------------
NO hidden modules were found.
NO system call table modifications were found.

WARNING: process id 13745 hidden or just exited (tb)
Launch Path: /root/code/interrogator/de·rojansans/tb
FOUND 1 Hidden process listing

HIDDEN File found: /tmp/hideme
WARNING: File size is 62629 (should be 61381): /var/log/sa/sa09
WARNING: File size is 1013693 (should be 1012816): /var/log/cron
WARNING: File size is 599450 (should be 599012): /var/log/maillog

HIDDEN TCP Port Listener found: port 2222
[root@localhost interrogator]# exit
```

FIG. 20(b)

```
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator... this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

-------------------------[ SUMMARY ]-------------------------
,WARNING suspect module found: f8a0f000 8000 bytes (adore)
'Image stored at /tmp/interrogator/adore.o
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[2]      FAILED   0xf8a0f650        fork
syscall[4]      FAILED   0xf8a0f7e8        write
syscall[5]      FAILED   0xf8a10184        open
syscall[6]      FAILED   0xf8a0f898        close
syscall[18]     FAILED   0xf8a0fbe4        oldstat
syscall[37]     FAILED   0xf8a0f710        kill
syscall[39]     FAILED   0xf8a0f9a0        mkdir
syscall[84]     FAILED   0xf8a0fcd0        oldlstat
syscall[106]    FAILED   0xf8a0fdbc        stat
syscall[107]    FAILED   0xf8a0fe94        lstat
syscall[120]    FAILED   0xf8a0f6b0        clone
syscall[141]    FAILED   0xf8a0f368        getdents
syscall[195]    FAILED   0xf8a0ff80        stat64
syscall[196]    FAILED   0xf8a10080        lstat64
syscall[220]    FAILED   0xf8a0f4dc        getdents64
Suspect module located (0xf89da6d8 - 0xf8a12000)
FOUND 15 Modified syscall table functions

WARNING: Found process id 836 removed from the task_queue.
Launch Path: /root/code/interrogator/demo/trojans/test
WARNING: process id 13745 hidden or just exited (tb)
Launch Path: /root/code/interrogator/demo/trojans/tb
FOUND 2 Hidden process listings

HIDDEN File found: /tmp/hideme
WARNING: File size is 2336990 (should be 2335392): /var/log/messages

HIDDEN TCP Port Listener found: port 111
HIDDEN TCP Port Listener found: port 139
HIDDEN TCP Port Listener found: port 2222
HIDDEN TCP Port Listener found: port 6000
HIDDEN TCP Port Listener found: port 32768
HIDDEN TCP Port Listener found: port 32769

[root@localhost interrogator]# exit
```

FIG. 20(c)

204

```
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator... this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

-------------------------[ SUMMARY ]-------------------------
WARNING suspect module found: f8a10000 184700 bytes (homegrown)
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[3]      FAILED   0xf8a11494        read
syscall[5]      FAILED   0xf8a11020        open
syscall[11]     FAILED   0xf8a10ebc        execve
syscall[13]     FAILED   0xf8a118a0        time
syscall[78]     FAILED   0xf8a1183c        gettimeofday
syscall[141]    FAILED   0xf8a11544        getdents
syscall[220]    FAILED   0xf8a116c0        getdents64
Suspect module located (0xf89db6d8 - 0xf8a3f000)
FOUND 7 Modified syscall table functions

WARNING: process id 1584 hidden or just exited (tb)
Launch Path: /root/code/interrogator/demo/trojans/tb
FOUND 1 Hidden process listing

HIDDEN File found: /tmp/hideme
WARNING: File size is 1021523 (should be 1020648): /var/log/cron
WARNING: File size is 603820 (should be 603384): /var/log/maillog

HIDDEN TCP Port Listener found: port 2222
[root@localhost interrogator]# exit
```

206

FIG. 20(d)